IN THE CLAIMS

Please amend the claims as follows:

1-23. (Cancelled)

24. (Currently amended) A method, comprising:

receiving, by a network adapter, a security association and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA);

generating, by said network adapter, a second integrity indicator based on said SA;

verifying, by said network adapter, that said SA within said network adapter is substantially similar and the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator; and

using said SA to decode ~~encode~~ data received from ~~for transmitting to~~ a network infrastructure device.

25. (Previously Presented) The method of claim 24, further comprising:

generating, by said IHA, said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and hash computations.

26. (Previously Presented) The method of claim 24, further comprising:

generating, by said network adapter, said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and hash computations.

27. (Previously Presented) The method of claim 24, further comprising:

indicating, by said network adapter, the integrity of said SA to said IHA.

28. (Previously Presented) The method of claim 24, further comprising:

setting an integrity error bit in a memory in the IHA.

29. (Currently amended) An apparatus comprising:

a network adapter comprising an integrated circuit, said integrated circuit is capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA), said integrated circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit being further capable of verifying that said SA received by said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator, said integrated circuit being further capable of using said SA to decode ~~encode~~ data received from ~~for transmitting to~~ a network infrastructure device.

30. (Previously Presented) The apparatus of claim 29, wherein:

said IHA being capable of generating said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and hash computations.

31. (Previously Presented) The apparatus of claim 29, wherein:

said integrated circuit being further capable of generating said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and hash computations.

32. (Previously Presented) The apparatus of claim 29, wherein:

said integrated circuit being further capable of indicating the integrity of said SA to said IHA.

33. (Previously Presented) The apparatus of claim 29, wherein:

said integrated circuit being further capable of setting an integrity error bit in a memory in the IHA.

34. (Currently amended) An article comprising:

a storage medium storing instructions that when executed by a machine result in the following operations:

receiving, by a network adapter, a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA;

generating, by said network adapter, a second integrity indicator based on said SA;

verifying, by said network adapter, that said SA within said network adapter is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator; and

using said SA to decode ~~encode~~ data received from ~~for transmitting to~~ a network infrastructure device.

35. (Previously Presented) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

generating, by said IHA, said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and hash computations.

36. (Previously Presented) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

generating, by said IHA, said network adapter, said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and ahs computations.

37. (Previously Presented) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

indicating, by said network adapter, the integrity of said SA to said IHA.

38. (Previously Presented) The article of claim 34, wherein said instructions that when executed by said machine result in the following additional operations:

setting an integrity error bit in a memory in the IHA.

39. (Currently amended) A system, comprising:

at least one network adapter being capable of being coupled to an information handling apparatus (IHA) via a bus, said network adapter comprising an integrated circuit capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by said IHA, said integrated circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator, said integrated circuit being further capable of using said SA to decode ~~encode~~ data received from ~~for transmitting to~~ a network infrastructure device.

40. (Previously Presented) The system of claim 39, wherein:

said IHA being capable of generating said first integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and hash computations.

41. (Previously Presented) The system of claim 39, wherein:

said integrated circuit being further capable of generating said second integrity indicator based on said SA using a data checking integrity method selected from the group consisting of: checksum, cyclical redundancy checking, Huffman coding, parity checking and hash computations.

42. (Previously Presented) The system of claim 39, wherein:

said integrated circuit being further capable of indicating the integrity of said SA to said IHA.

43. (Previously Presented) The system of claim 39, wherein:

said integrated circuit being further capable of setting an integrity error bit in a memory in the IHA.